AMENDMENTS TO THE CLAIMS

1-34. **(Canceled)**

35. **(Previously Presented)** A copyright protection system comprising:

a recording apparatus configured to encrypt a content and to record the encrypted content;

a recording medium on which the encrypted content is recorded; and

a plurality of reproduction apparatuses, each of which is configured to read out and decrypt the encrypted content recorded on said recording medium,

wherein each of said plurality of reproduction apparatuses is one of either a first plurality of reproduction apparatuses which belong to a first category and hold plural device keys in association with information regarding generations of the plural device keys or a second plurality of reproduction apparatuses which belong to a second category and hold only one device key, the plural device keys including a device key held since before and a device key provided in response to when revocation stops functioning,

said recording apparatus is configured (a) to generate, for said plurality of reproduction apparatuses and based on a media key and a device key held by each of said plurality of reproduction apparatuses, a plurality of revocation data intended for revoking a device key held by a specific reproduction apparatus of a respective category, (b) to generate the encrypted content which is the content encrypted based on the media key, and (c) to record the plurality of revocation data, information regarding t a generation of the device key for generating each of the plurality of revocation data, and the encrypted content onto said recording medium,

the first plurality of reproduction apparatuses are each configured (a) to read out, from said recording medium, the plurality of revocation data corresponding to said first plurality of reproduction apparatuses, the information regarding the generations of the device key, and the encrypted content, and (b) to decrypt the encrypted content based on the plurality of revocation data read out and the information regarding the generation of the device key,

the second plurality of reproduction apparatuses are each configured (a) to read out, from said recording medium, the plurality of revocation data corresponding to said second plurality of

reproduction apparatuses and the encrypted content, and (b) to decrypt the encrypted content based on the plurality of revocation data read out,

each one of the plurality of revocation data is encrypted media key data which is the media key encrypted using a device key held by said plurality of reproduction apparatuses of a corresponding category,

the first plurality of reproduction apparatuses are each configured (a) to read out, from said recording medium, the corresponding encrypted media key data, the information regarding the generation of the device key, and the encrypted content, (b) to select a device key associated with the information regarding the generation of the device key, from among the held plural device keys (c) to obtain the media key by decrypting the encrypted media key data using the selected device key, and (d) to decrypt the encrypted content based on the obtained media key, and

the second plurality of reproduction apparatuses are each configured (a) to read out, from said recording medium, the corresponding encrypted media key data and the encrypted content, (b) to obtain the media key by decrypting the encrypted media key data using the held device key, and (c) to decrypt the encrypted content based on the obtained media key.

36. **(Canceled)**

37. **(Previously Presented)** The copyright protection system according to Claim 35,

wherein said recording apparatus is configured to generate an encryption key based on the media key, and to encrypt the content based on the encryption key, and

said plurality of reproduction apparatuses of the respective categories are each configured to generate a decryption key based on the obtained media key, and to decrypt the encrypted content based on the generated decryption key.

38. **(Previously Presented)** The copyright protection system according to Claim 35,

wherein said recording apparatus is configured to encrypt the content using a content key,

to generate encrypted content key data by encrypting the content key using the media key, and to record the generated encrypted content key data onto said recording medium, and

said plurality of reproduction apparatuses of the respective categories are each configured to read out the encrypted content key data from said recording medium, to obtain the content key by decrypting the encrypted content key data using the media key, and to decrypt the encrypted content using the obtained content key.

39. **(Previously Presented)** The copyright protection system according to Claim 35,

wherein each one of the plurality of revocation data is encrypted media key data which is a media key for a corresponding category, encrypted using the device key data held by said plurality of reproduction apparatuses of a corresponding category,

said recording apparatus is configured to encrypt the content using a content key, to generate a plurality of encrypted content key data by encrypting the content key using the media key corresponding to the category of said plurality of reproduction apparatuses, and to record, onto said recording medium, at least encrypted media key data, the information regarding a generation of the device key for encrypting the media key, the plurality of encrypted content key data, and the encrypted content,

the first plurality of reproduction apparatuses are each configured (a) to read out, from said recording medium, the information regarding the generation of the device key, the encrypted media key data for the corresponding category, the encrypted content key data for the corresponding category, and the encrypted content, (b) to select a device key associated with the information regarding the generation of the device key, from among the held plural device keys, (c) to obtain a media key for the corresponding category by decrypting the encrypted media key data using the selected device key, (d) to obtain the content key by decrypting the encrypted content key data for the corresponding category using the obtained media key for the corresponding category, and (e) to decrypt the encrypted content using the obtained content key, and

the second plurality of reproduction apparatuses are each configured (a) to read out, from

said recording medium, the encrypted media key data for the corresponding category, the encrypted content key data for the corresponding category, and the encrypted content, (b) to obtain the media key for the corresponding category by decrypting the encrypted media key data using the held device key, (c) to obtain the content key by decrypting the encrypted content key data for the corresponding category using the obtained media key for the corresponding category, and (d) to decrypt the encrypted content using the obtained content key.

40. **(Previously Presented)** The copyright protection system according to Claim 35,

wherein each one of the plurality of revocation data is encrypted media key data which is a media key for a corresponding category, encrypted using the device key held by said plurality of reproduction apparatuses of a corresponding category,

each of the first plurality of reproduction apparatuses includes:

a read-out apparatus of the second category configured to read out and perform a part of a decryption process on the encrypted content recorded on said recording medium; and

a decryption apparatus of the first category, connected to said read-out apparatus of the second category, configured to perform a part of the decryption process on the encrypted content,

said recording apparatus is configured (a) to generate, based on a media key and on a device key held by each of said decryption apparatuses of the first category, a plurality of first encrypted media key data intended for revoking a device key held by a specific decryption apparatus of the first category, (b) to generate, based on a media key and on a device key held by each of apparatuses of the second category, a plurality of second encrypted media key data intended for revoking a device key held by a specific apparatus of the second category, (c) to generate an encrypted content which is the content encrypted based on the media key, and (d) to record at least the plurality of first encrypted media key data, information regarding a generation of the deice key for generating each of the plurality of first encrypted media key data, the plurality of second encrypted media key data, and the encrypted content onto said recording medium,

the second plurality of reproduction apparatuses are each configured to read out the

plurality of second encrypted media key data and the encrypted content from said recording medium, to obtain the media key by decrypting the plurality of second encrypted media key data using the held device key, and to decrypt the encrypted content based on the obtained media keyt, and

in each of the first plurality of reproduction apparatuses:

said read-out apparatus of the second category is configured (a) to read out, from said recording medium, the plurality of first encrypted media key data, the information regarding the generation of the device key, the plurality of second encrypted media key data, and the encrypted content, and (b) to supply intermediate data, the information regarding the generation of the device key, and the plurality of first encrypted media key data to said decryption apparatus of the first category, the intermediate data being the encrypted content on which a part of the decryption process has been performed based on the plurality of second encrypted media key data; and

said decryption apparatus of the first category is configured to hold plural device keys in association with information regarding generations of the plural device keys, to select a device key associated with the information regarding the generation of the deice key supplied by said read-out apparatus of the second category, to obtain the media key by decrypting the plurality of first encrypted media key data using the selected device key, and to obtain the content by performing the decryption process on the intermediate data based on the obtained media key, the plural device keys including a device key held since before and a device key provided in response to when revocation stops functioning.

41. **(Previously Presented)** A recording apparatus which encrypts a content and records the encrypted content, the content being reproduced by first reproduction apparatuses which belong to a first category and hold plural device keys in association with information regarding generations of the plural device keys and by second reproduction apparatuses which belong to a second category and hold only one device key, the plural device keys including a device key held since before and a device key provided in response to when revocation stops functioning,

wherein said recording apparatus (a) generates, for a plurality of reproduction

apparatuses and based on a media key and a device key held by each of the plurality of reproduction apparatuses, a plurality of revocation data intended for revoking a device key held by a specific reproduction apparatus belonging to respective categories, (b) generates an encrypted content which is the content encrypted based on the media key, and (c) records the plurality of revocation data, the information regarding the generation of the device key for generating each of the plurality of revocation data, and the encrypted content onto a recording medium,

the plurality of revocation data includes first revocation data generated based on a device key selected from among the plural device keys held by said first reproduction apparatuses and second revocation data generated based on the device key held by said second reproduction apparatuses.

42. **(Previously Presented)** The recording apparatus according to Claim 41,

wherein each one of the plurality of revocation data is encrypted media key data which is the media key encrypted using the device key held by the plurality of reproduction apparatuses of a corresponding category.

43. **(Previously Presented)** The recording apparatus according to Claim 42,

wherein said recording apparatus generates an encryption key based on the media key, and encrypts the content based on the encryption key.

44. **(Previously Presented)** The recording apparatus according to Claim 42,

wherein said recording apparatus encrypts the content using a content key, generates encrypted content key data which is the content key encrypted using the media key, and records the generated encrypted key onto the recording medium.

45. **(Previously Presented)** The recording apparatus according to Claim 41,

wherein each one of the plurality of revocation data is encrypted media key data which is

a media key for a corresponding category, encrypted using the device key held by the plurality of reproduction apparatuses of the corresponding category, and

said recording apparatus is configured (a) to encrypt the content using a content key, (b) to generate a plurality of encrypted content key data by encrypting the content key using the media keys corresponding to the category of the reproduction apparatus, and (c) to record, onto the recording medium, at least the encrypted media key data, the information regarding the generation of the device key for encrypting the media key, the plurality of encrypted content key data, and the encrypted content.

46. **(Previously Presented)** The recording apparatus according to Claim 41,

wherein said recording apparatus (a) generates, based on a media key and on a device key held by each of decryption apparatuses of the first category, a plurality of first revocation data intended for revoking a device key held by a specific decryption apparatus of the first category, (b) generates, based on a media key and on a device key held by apparatuses of the second category, a plurality of second revocation data intended for revoking a device key held by a specific apparatus of the second category, and (c) generates an encrypted content which is the content encrypted based on the media key, and (d) records at least a plurality of first revocation data, information regarding the generation of the device key for generating each of the plurality of first revocation data, a plurality of the second revocation data, and the encrypted content onto the recording medium.

47. **(Previously Presented)** A recording medium on which a content reproduced by a plurality of reproduction apparatuses is recorded, the plurality of reproduction apparatuses including first reproduction apparatuses belonging to a first category and holding plural device keys in association with information regarding generations of the plural device keys, and second reproduction apparatuses belonging to a second category and holding only one device key, the plural device keys including a device key held since before and a device key provided in response to when revocation stops functioning,

wherein on said recording medium, at least (i) a plurality of revocation data generated based on a media key a the device key held by each of the plurality of reproduction apparatuses and intended for revoking the device key held by the specific reproduction apparatus of the respective categories, (ii) information regarding a generation of the device key for generating each of the plurality of revocation data, and (iii) an encrypted content generated by encrypting the content based on the media key are recorded, and

the plurality of revocation data includes first revocation data includes first revocation data generated based on a device key selected from among the plural device keys held by said first reproduction apparatuses and second revocation data generated based on the device key held by said second reproduction apparatuses.

48. **(Previously Presented)** The recording medium according to Claim 47,

wherein each one of the plurality of revocation data is encrypted media key data which is the media key encrypted using the device key held by the plurality of reproduction apparatuses of a corresponding category.

49. **(Previously Presented)** The recording medium according to Claim 48,

wherein the encrypted content is generated by encrypting the content, based on an encryption key generated based on the media key.

50. **(Previously Presented)** The recording medium according to Claim 48,

wherein the encrypted content is generated by encrypting the content using a content key, and

on said recording medium, encrypted content key data is recorded, the encrypted content key data being generated by encrypting the content key using the media key.

51. **(Previously Presented)** The recording medium according to Claim 47,

wherein each one of the plurality of revocation data is encrypted media key data which is

a media key for a corresponding category, encrypted using the device key held by the plurality of reproduction apparatuses of the corresponding category,

the encrypted content is generated by encrypting the content using a content key, and

on said recording medium, a plurality of encrypted content key data generated by encrypting the content key using the media keys corresponding to the category of the plurality of reproduction apparatuses are recorded.

52. **(Previously Presented)** The recording medium according to Claim 47,

wherein on said recording medium, at least (i) a plurality of first revocation data generated based on the media key and on a device key held by each of decryption apparatuses of the first category and intended for revoking a device key held by a specific decryption apparatus of the first category, (ii) information regarding a generation of the device key for generating the plurality of first revocation data, (iii) a plurality of second revocation data generated based on a media key and on a device key held by each of apparatuses of the second category and intended for revoking a device key held by a specific apparatus of the second category, and (iv) the encrypted content which is the content on which an encryption process has been performed based on the media key are recorded.

53. **(Previously Presented)** A computer-readable recording medium on which a program causing a computer to reproduce an encrypted content is recorded,

wherein on said recording medium, at least revocation data generated based on a media key and a device key held by the computer and intended for revoking the device key held by the computer, an encrypted content generated by encrypting a content based on the media key, and information regarding a generation of the device key for generating the revocation data are recorded,

the revocation data is encrypted media key data which is the media key encrypted using the device key held by the computer, and

the program recorded on said recording medium causes the computer which holds plural

device keys in association with information regarding generations of the plural device keys (a) to read out, from the recording medium, the corresponding encrypted media key data, the information regarding the generation of the deice key, and the encrypted content, (b) to select a device key associated with the information regarding the generation of the device key, from among the held plural device keys, (c) to obtain the media key by decrypting the encrypted media key data using the selected device key, and (d) to decrypt the encrypted content based on the obtained media key, the plural device keys including a device key held since before and a device key provided in response to when revocation stops functioning

54. **(Canceled)**

55. **(Previously Presented)** The recording medium according to Claim 53,

wherein the encrypted content is generated by encrypting the content, based on an encryption key generated based on the media key, and

the program recorded on said recording medium causes the computer to generate a decryption key based on the obtained media key, and to decrypt the encrypted content based on the generated decryption key.

56. **(Previously Presented)** The recording medium according to Claim 53,

wherein the encrypted content is generated by encrypting the content using a content key,

on the recording medium, encrypted content key data generated by encrypting the content key using the media key is recorded, and

the program recorded on said recorded medium causes the computer (a) to read out the encrypted content key data from the recording medium, (b) to obtain the content key by decrypting the encrypted content key data using the media key, and (c) to decrypt the encrypted content using the obtained content key.

57. **(Previously Presented)** The recording medium according to Claim 53,

wherein the revocation data is encrypted media key data which is a media key for a corresponding category, encrypted using the device key held by the computer,

the encrypted content is generated by encrypting the content using a content key,

on the recording medium, a plurality of encrypted content key data generated by encrypting the content key using the media keys corresponding to the category of the computer is recorded, and

the program recorded on said recording medium causes the computer (a) to read out, from the recording medium, the encrypted media key data for the corresponding category, the encrypted content key data for the corresponding category, the encrypted content, and the information regarding the generation of the device key, (b) to select a device key associated with the information regarding the generation of the device key, from among the held plural device keys, (c) to obtain the media key for the corresponding category by decrypting the encrypted media key data using the selected device key, (d) to obtain the content key by decrypting the encrypted content key data using the obtained media key for the corresponding category, and (e) to decrypt the encrypted content using the obtained content key.

58. **(Previously Presented)** The recording medium according to Claim 53,

wherein on the recording medium, at least (i) a plurality of first revocation data generated based on the media key and on a device key held by each of decryption apparatuses of a first category and intended for revoking a device key held by a specific decryption apparatus of the first category, (ii) information regarding a generation of the device key for generating the plurality of first revocation data, (iii) a plurality of second revocation data generated based on a media key and on a device key held by each of apparatuses of a second category and intended for revoking a device key held by a specific apparatus of the second category, and (iv) the encrypted content which is the content on which an encryption process has been performed based on the media key are recorded, and

the program recorded on said recording medium causes the computer which belongs to the second category to read out, from the recording medium, the plurality of second revocation

data and the encrypted content, and to decrypt the encrypted content based on the plurality of second revocation data.

59. **(Previously Presented)** The recording medium according to Claim 58,

wherein the program recorded on said recording medium causes:

a read-out apparatus belonging to the second category to read out, from the recording medium, the plurality of first revocation data, the plurality of second revocation data, the information regarding the generation of the device key, and the encrypted content, to generate intermediate data which is the encrypted content on which a part of a decryption process has been performed based on the plurality of second revocation data, and to output the generated intermediate data, the information regarding the generation of the device key, and the plurality of first revocation data; and

a decryption apparatus belonging to the first category to obtain the content by performing a decryption process on the intermediate data, based on the plurality of first revocation data and the information regarding the generation of the device key outputted by the read-out apparatus belonging to the second category.

60. **(Currently Amended)** A copyright protection system comprising:

a key generation apparatus configured to generate and record a plurality of revocation data necessary for encrypting and decrypting a content,

a plurality recording apparatuses, each of which is configured to encrypt a content and to record the encrypted content;

a recording medium on which the encrypted content and the plurality of revocation data are recorded; and

a plurality of reproduction apparatuses, each of which is configured to read out and decrypt the encrypted content recorded on said recording medium,

wherein each of said plurality of reproduction apparatuses is one of either first reproduction apparatuses which belong to a first category and hold plural device keys in

association with information regarding generations of the plural device keys or second reproduction apparatuses which belong to a second category and hold only one device key, the plural device keys including a device key held since before and a device key provided in response to when revocation stops functioning,

each of said plurality ~~recording apparatuses~~ of reproduction apparatuses belongs to either the first category or the second category,

said key generation apparatus is configured (a) to generate, for said plurality of reproduction apparatuses and based on a media key and a device key held by each of said plurality recording apparatuses or plurality of reproduction apparatuses, the plurality of revocation data intended for revoking a device key held by a specific recording apparatus or a specific reproduction apparatus of the respective categories, and (b) to record the generated a plurality of revocation data and the information regarding a generation of the device key for generating the plurality of revocation data onto said recording medium,

said plurality recording apparatuses are each configured (a) to read out, from said recording medium, the plurality of revocation data for the category to which said recording apparatus belongs, (b) to generate the encrypted content by encrypting the content based on the plurality of revocation data read out, and (c) to record the generated encrypted content on said recording medium,

each one of the plurality of revocation data is encrypted media key data which is the media key encrypted using a device using a device key held by the reproduction apparatus of a corresponding category

the first reproduction apparatuses are each configured (a) to read out, from said recording medium, the corresponding encrypted media key data, the information regarding the generation of the device key, and the encrypted content, and (b) to select a deice key associated with the information regarding the generation of the device key, from among the held plural device keys, (c) to obtain the media key by decrypting the encrypted media key data using the selected device key, and (d) to decrypt the encrypted content based on the obtained media key, and

the second reproduction apparatuses are each configured (a) to read out, from said

recording medium, the plurality of revocation data corresponding to said second reproduction apparatus and the encrypted content, and (b) to decrypt the encrypted content based on the plurality of revocation data read out.

61. **(Previously Presented)** A recording method for use in a recording apparatus which encrypts a content reproduced by plurality of reproduction apparatuses and records the encrypted content, the plurality of reproduction apparatuses including first reproduction apparatuses belonging to a first category and holding plural device keys in association with information regarding generations of the plural device keys, and second reproduction apparatuses belonging to a second category and holding only one device key, the plural device keys including a device key held since before and a device key provided in response to when revocation stops functioning, said method comprising:

a step of generating, for the plurality of reproduction apparatuses and based on a media key and a device key held by each of the plurality of reproduction apparatuses, a plurality of revocation data intended for revoking a device key held by a specific reproduction apparatus of the respective categories;

an encrypted content generation step of generating the encrypted content by encrypting the content, based on the media key; and

a recording step of recording the plurality of revocation data, the information regarding a generation of the device key for generating each of the plurality of revocation data, and the encrypted content onto the recording medium.

62. **(Previously Presented)** A reproduction method for use in a reproduction apparatus which belongs to one of plural categories, holds plural device keys in association with information regarding generations of the plural device key, and reproduces an encrypted content recorded on a recording medium, the plural device keys including a device key held since before and a device key provided in response to when revocation stops functioning,

wherein on the recording medium, at least a plurality of revocation data generated based

on a media key and a device key held by the reproduction apparatus and intended for revoking the device key held by the reproduction apparatus, the encrypted content generated by encrypting a content based on the media key, and information regarding a generation of the device key are recorded,

each one of the plurality of revocation data is encrypted media key data which is the media key encrypted using a device key held by the reproduction apparatus of a corresponding category,

said reproduction method comprises:

a read-out step of reading out, from the recording medium the corresponding encrypted media key data, the generation of the device key, and the encrypted content; and

a decryption step of selecting a device key associated with the information regarding the generation of the device key, from among the held plural device keys, obtaining the media key by decrypting the encrypted media key data using the selected device key, and decrypting the encrypted content based on the obtained media key.